GDPR

Action Research Session

Plan or implementation

12 steps to prepare for gdpr

12 steps to prepare for gdpr

- 1. ***Awareness*** – SLT, Governors etc. need to appreciate the impact this is likely to have
- 2. ***Information you hold*** – document what personal data you hold etc. Data flows/data audits
- 3. ***Privacy Notices*** – review and update what you have already and plan for any necessary changes
- 4. ***Individual's rights*** – do you comply with all their rights? Data deletion? Withdrawn consent?
- 5. ***Subject Access Requests*** – update or develop procedures for these so you are ready
- 6. ***Lawful basis for processing*** – identify the legal basis for your processing of personal data. Document the legal basis and update privacy notices to explain it.

12 steps to prepare for gdpr

- 7. ***Consent*** – if you need consent for any processing, how are you going to get it, record it, refresh existing consents etc.?
- 8. ***Children*** – parental consent up to 13 years of age, thereafter the pupil's own consent. How are you going to manage this?
- 9. ***Data breaches*** – procedures in place? Whose responsibility etc.?
- 10. ***Privacy Impact Assessments*** – good practice to have these for all processing and then update if processes or technology changes or new processing being considered
- 11. ***DPO*** – decide who it is going to be and appoint asap so they can help get ready for GDPR
- 12. ***International*** – do you know where personal data is going? Suppliers? Cloud software?

Data protection officer

Data protection officer

- Every school will need to appoint a DPO, whose responsibilities include:

- *To inform & advise the organisation* and its employees about their obligations to comply with GDPR and other data protection laws
- *To monitor compliance with GDPR* and other data protection laws, including managing internal data protection activities, advise on data protection impact assessments; train staff and conduct internal audits
- To be the first point of contact for the ICO and for individuals whose data is processed (staff, pupils, parents etc.)

Data protection officer

- Must report to the highest management level of your organisation
- Operate independently and cannot be dismissed or penalised for performing their task
- Have adequate resources to enable them to meet their GDPR obligations
- *No conflicts of interest*
- Must have professional experience and knowledge of data protection law
- *Who will be your DPO?*
- Internal staff member / new role recruited / shared / external ?

accountability

accountability

- Need to have in place comprehensive, proportionate governance measures
- *'Appropriate technical and organisational measures that ensure and demonstrate that you comply'*
- Privacy by design – at the front of your mind whenever considering new processes or technology
- Privacy Impact Assessments / Data Protection Impact Assessments
- Data minimisation – only process what you actually need
- Measures to minimise risk of breaches & uphold protection of personal data
- Deletion of data when no longer needed
- Records of processing activities (what, why, DPO, retention policy, description of security etc.)

accountability

- Regular and relevant staff training
- Processes and procedures in place and documented
- Evidence that these are understood by staff
- Evidence that staff understand their DP responsibilities
- Regular monitoring and audits undertaken
- Issues discovered and acted upon
- Regular agenda item on SLT meetings
- *Demonstrating accountability is key to GDPR compliance*

Privacy by design

- *Express legal requirement under GDPR*
- Need to have this in place and be able to evidence it too
- Staff training (with records to evidence it)
- Data security policies in place setting out how you will always have privacy in mind
- DPIA for all processes / new technologies etc.
- Results may mean changes…
- Appropriate resources provided to affect the changes necessary

Third party processors

Activity 1 - Think about & list the types of suppliers you use?

- Cashless catering, library systems, parental communications, behaviour software etc.
- Payroll, healthcare, pensions etc.
- Data controller *(you)* are responsible for ensuring compliance
- Data processor also has to be compliant
- Both parties have to keep records of the processing activities
- Processors can only be used under a legally binding contract

What processing might we need consent for?

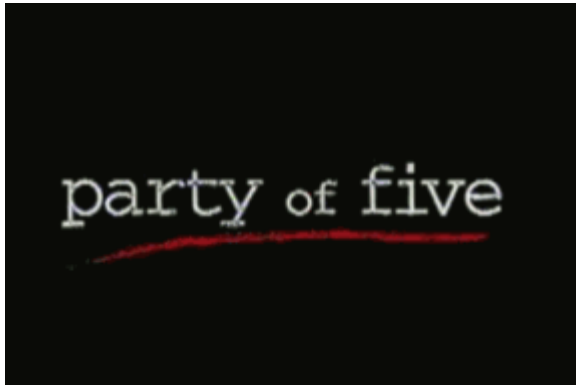
Activity 2 - Think about & list the types of processes you might need consent for?

- External, third-party suppliers?
- Sharing data with other agencies?
- Sharing data with other schools?
- School photography companies?
- Anything that a parent, pupil, governor, member of staff etc. might not reasonably expect us to be doing with their data

Staff training

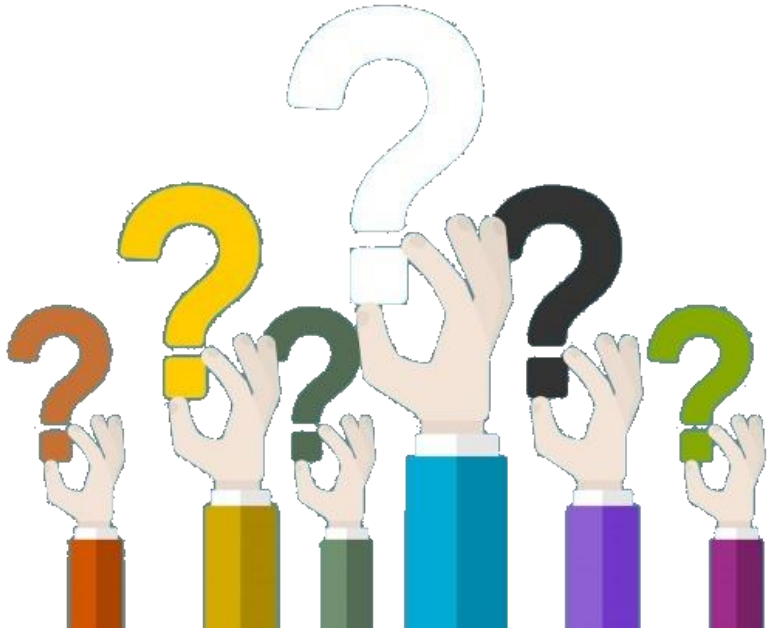
Activity 3 - Think about whose that'll need training & document the process?

- Regular and relevant staff training
- Processes and procedures in place and documented
- Evidence that these are understood by staff
- Evidence that staff understand their DP responsibilities
- Regular monitoring and audits undertaken
- Issues discovered and acted upon
- Regular agenda item on SLT meetings
- *Demonstrating accountability is key to GDPR compliance*



Plan to re-convene at BETT to share best practice

Questions?



Thank you

Stuart Abrahams

Email: stuart.abrahams@think-it.org.uk
Mob: 07907 50 7777
Skype: stuartabrahams